UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

5020 Simpson Drive,
Sanford, North Carolina 27330

Case No. 1:19-mj-132

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The premises located at 5020 Simpson Drive, Sanford, North Carolina 27330, more particularly described in Attachment A.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), all of which are more particularly described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(a)(2)(A)	Distribution/Receipt of Child Pornography
18 U.S.C. §§ 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jessica Smeltz
Applicant's signature

Special Agent Jessica Smeltz, FBI
Printed name and title

Pursuant to Rule 4.1 of the Federal Rules of Criminal Proceedure, the applicant appeared before me via reliable electronic means and was placed under oath.

Date: 4/19/19 12:20 pm

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jessica Smeltz, a Special Agent (SA) with the Federal Bureau of Investigation (FBI) being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating the trafficking of child pornography via a peer-to-peer network at an address in Lee County, North Carolina.

2. This affidavit is submitted in support of an application for a warrant to search the location described in Attachment A, the premises located at 5020 Simpson Drive, Sanford, North Carolina 27330 (the "SUBJECT PREMISES"), for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2)(A), which items are more specifically described in Attachment B of this Affidavit.

3. The information contained within this affidavit is based on my training and experience, as well as information I have developed and information relayed to me by other law enforcement agencies. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this

investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that instrumentalities, fruits and evidence of violations of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2)(A) are located at the SUBJECT PREMISES.

AGENT BACKGROUND

4. I am a Special Agent (SA) of Federal Bureau of Investigation ("FBI"), and have been since March of 2017. I am currently assigned to the Fayetteville Resident Agency of the Charlotte, North Carolina Division. I am assigned to the Violent Crimes Against Children Unit where I am responsible for investigations involving the production, advertisement, receipt, distribution, and possession of child pornography. I am a graduate of the twenty one week FBI Basic Field Training Course for special agents in Quantico, Virginia. I have received training in the area of child pornography and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and child pornography crimes. I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256.

5. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A and 2251, and I am authorized by the Attorney General to request a search warrant.

STATUTORY AUTHORITY

6. This investigation concerns violations of 18 U.S.C. § 2252A relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

b. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign

commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

DEFINITIONS

7. The following definitions apply to this application:

a. "Child Pornography," is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. "Visual Depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

c. "Sexually Explicit Conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal),

whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

d. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

e. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

f. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. Internet Protocol Address" or "IP Address" is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a

range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Secure Hash Algorithm" (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm as a Federal Information Processing Standard. SHA1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

i. "Computer" refers to an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or

communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

j. "Storage Medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

k. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

l. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer

software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

m. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

n. "Records" and "Information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any

photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

THE BITTORRENT PEER-TO-PEER NETWORK

8. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that millions of computer users throughout the world use peer-to-peer (P2P) file sharing networks to share files containing music, graphics, movies, and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

9. The BitTorrent network is a publicly available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

10. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, µTorrent client program, and Vuze client program, among others. These client programs are publically

available and typically free software programs that can be downloaded from the Internet.

11. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. This is commonly referred to as "passive distribution."

12. As an example, during the downloading and installation of the publically available µTorrent client program, the license agreement for the software states the following: "Automatic Uploading. µTorrent accelerates downloads by enabling your computer to grab pieces of files from other µTorrent or BitTorrent users simultaneously. Your use of the µTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In µTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall µTorrent through the Add/Remove Programs control panel utility. In addition, you can control µTorrent in multiple ways through its user interface without affecting any files you have already downloaded."

13. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding."

14. Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash" is a SHA1 hash value of the set of data describing the file(s) referenced in the "Torrent." This set of data includes the SHA1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s)

referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent." "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing.

15. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

16. In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and thepiratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the

"Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file.

17. It is again important to note that the actual file(s) referenced in the "Torrent" are obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the Internet Protocol (IP) addresses of the remote peers/clients.

18. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing

website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program on their computer will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients would then be located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files to the user's computer.

19. Typically, once the BitTorrent network client has downloaded part of a file or files, it will immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA1 piece hash described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

20. Law enforcement efforts have resulted in the creation of BitTorrent network client programs that obtain information from "Trackers"

about peers/clients on the BitTorrent network involved in sharing digital files of known or suspected child pornography. This is accomplished using based on "info hash" SHA1 hash values of "Torrents" which have been previously identified by law enforcement as being associated with such files. The law enforcement BitTorrent network client programs are designed to perform single-source downloads of files. In other words, entire files are downloaded from a single computer at a single IP address.

21. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be shared by the suspect client program with the law enforcement BitTorrent client program. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, and that the pieces are being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer.

22. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. P2P investigative methodology has led to the issuance

and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the active hands-on sexual exploitation of actual children.

SUMMARY OF THE INVESTIGATION

23. As part of undercover investigations, law enforcement agents around the country have devised a number of proactive investigative techniques aimed at identifying and investigating individuals involved in the trafficking of child pornography. One such technique is the use of undercover investigative software on peer-to-peer networks to automate the browsing of suspected child pornography files and any subsequent download by law enforcement.

24. On February 14, 2019, a computer assigned to an FBI agent in the Charlotte Division was connected to the BitTorrent peer-to-peer network and observed that an individual with IP address 172.220.228.246 was offering to distribute file(s) associated with a particular torrent file (info hash of 8ee07b18029056202c8825e133532a67d0f5ec03). This torrent file identifies forty files, at least one of which has previously been identified as being of interest to child pornography investigations.

25. From February 14, 2019 through April 3, 2019, the FBI computer directly downloaded more than 100 files from an individual at IP address 172.220.228.246 via the BitTorrent peer-to-peer network. I have reviewed many of these files and many are child pornography. A selection of several follows:

File Name: PTHC_7yo_sex_in_serial_Hussyfan_R_ygold_6yo
Description: A video that is approximately 1 minute and 17 seconds long that depicts an adult male engaging in vaginal sex with a minor female who appears to be under the age of 7.
Download Date: 02/15/2019 [3:29 AM]

File Name: 12YO Emma (Blowjob Adair Part 2) (Resized) (2011)
Description: A video that is approximately 16 seconds long that depicts a minor female who appears to be under the age of 12, giving oral sex to an adult male. The minor female is wearing a blindfold that has the word "cock" among other words written on it.
Download Date: 02/14/2019 [3:29 AM]

File Name: toddler being fucked by man 78678 (2) (2) (2)
Description: A video that is approximately 7 seconds long that depicts an adult male having vaginal sex with a minor female who appears to be under the age of 2.
Download Date: 02/16/2019 [6:32 PM]

File Name: papa t babyj 5yr assfuck (2) (2) (2) (2)

Description: A video that is approximately 45 seconds long that depicts an adult male having anal sex with a minor female who appears to be under the age of 4. As the video progresses, the adult male has vaginal sex with the minor female.

Download Date: 02/16/2019 [6:32 PM]

File Name: (pthc) slave play_w-sound 4 yo cries, squirms

Description: A video that is approximately 3 minutes and 8 seconds long that depicts a minor female, who appears to be under the age of 3, laying on her back. She is wearing only a diaper and a black mask. An adult male, also wearing a black mask, is observed kissing the minor female on the lips. As the video progresses, the adult male exposes the child's genitals and digitally penetrates her vagina. The adult male then places his penis in her vagina before having the minor female perform oral sex on him.

Download Date: 02/16/2019 [6:32 PM]

File Name: ! new ! (pthc) 2007 tara 8yr - ass fuck and ass vibrator

Description: A video that is approximately 19 seconds long and depicts an adult male having anal sex with a minor female who appears to be under the age of 10.

Download Date: 03/07/2019 [3:12 AM]

File Name: Pthc Toddler Girl Daphne Diaper (Tender) Bum Yum Diaper Baby Babyshivid Pedo 1Yo 2Yo 3Yo 4Yo 5Yo Private Incest Toddler Avi

Description: A video that is approximately 4 minutes and 24 seconds long and depicts an adult male and a minor female who appears to be under the age of 2. The adult male removes the child's diaper and digitally penetrates the child, and preforms oral sex on the

child. As the video progresses, the adult male rubs his penis on the child's genitals and ejaculates on the child's genitals.

Download Date: 03/07/2019 [3:48 AM]

File Name: 23716be71968e657598c9322487d8b1f – 2012 anal girl man pthc sound

Description: A video that is approximately 24 seconds long and depicts an adult male having anal sex with a minor female who appears to be under the age of 10.

Download Date: 04/02/2019 [2:41AM]

26. A records check was conducted on IP address 172.220.228.246 through the American Registry for Internet Numbers (ARIN). The IP address was shown to belong to Charter Communications. Records obtained from Charter Communications revealed that, from February 14, 2019 to February 20, 2019, IP address 172.220.228.246 was assigned to the following subscriber:

Subscriber Name:	Wayne Bowen
Subscriber Address:	5020 Simpson Dr., Sanford, NC 27330
Activate Date:	September 15, 2018

27. A records check was conducted on IP address 172.220.228.246 through the American Registry for Internet Numbers (ARIN). The IP address was shown to belong to Charter Communications. Records obtained from

Charter Communications revealed that, from February 23, 2019 to April 03, 2019, IP address 172.220.228.246 was assigned to the following subscriber:

Subscriber Name: Wayne Bowen

Subscriber Address: 5020 Simpson Drive, Sanford, NC 27330

Activate Date: September 15, 2018

28. A search of the North Carolina Division of Motor Vehicles revealed that the following four individuals list their address as 5020 Simpson Drive, Sanford, North Carolina 27330 (the SUBJECT PREMISES):

Wayne Bowen, DOB: 12/27/1949

Suzanne Bowen, DOB: 2/27/1950

John Bowen, DOB: 3/5/1980

Christopher Bowen, DOB: 5/2/2002

29. On February 26, 2019 and April 12, 2019, physical surveillance was conducted on the SUBJECT PREMISES. On both dates multiple vehicles were parked at the SUBJECT PREMISES. The numbers "5020" can be seen on the mail box post.

BACKGROUND ON THE INTERNET, COMPUTERS, AND CHILD PORNOGRAPHY

30. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know the following about computer-related child exploitation crimes:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital images can be produced using a variety of devices including digital cameras, laptop/desktop computers, and mobile devices. Unlike traditional photography, digital photography typically allows a user to easily and inexpensively take and store large quantities of images. In fact, once a device is purchased there is no expense associated with capturing images.

c. With today's technology, digital images can be easily transferred between a user's devices and among individuals. Internet Service Providers enable users to connect to the Internet through a variety of means such as cable, Wi-Fi, and cellular service. Electronic contact can

be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. Child pornography can be transferred via peer-to-peer networks, email, MMS text message, mobile messaging applications, cloud storage services, and webpage bulletin boards to anyone with access to a computer and the Internet. Individuals interested in the sexual exploitation of children use technology to exchange child pornography with each other and to transfer their child pornography between their devices.

d. Individuals interested in the sexual exploitation of children may also use technology to target minors, interact with minors, and entice minors to produce child pornography. This is often accomplished through the use of social networking applications such as Facebook, Instagram, Kik Messenger, Musical.ly, and LiveMe.

e. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last

several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it to any one of the mentioned media storage devices. Media storage devices can easily be concealed and carried on an individual's person. Mobile devices, such as smartphones, are also often carried on an individual's person.

f. Cloud storage services are further changing how electronic data is stored. These services, such as Dropbox, Box, and Google Photos, and Google Drive enable a user to store data on remote services and access it on any of their computers by using installed applications/software. A user can also access their data via an Internet Browser from any computer with an Internet connection. Cloud storage services provide a convenient way to share data with others. Recently, this has become a particularly

popular way to share child pornography. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer or external media in most cases.

g. Mobile devices are hand-held computers that can transfer media through multiple methods – cellular signal, Wi-Fi, Bluetooth, and near field communication (NFC). In addition, mobile devices are commonly set to backup automatically when connected to a computer. Individuals have been known to plug their mobile devices into computers causing data to be backed up to the computer without even realizing that this data transfer is occurring. Mobile devices can also be set to sync automatically with Cloud storage and paired devices. For example, an individual using Google Photos or iCloud Photo Library may have images taken using a mobile device automatically backup to cloud storage and pushed out to, or "synced," with their other computer devices.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files).

Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., application data, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

31. As described in Attachment B, this application seeks permission to search for records and information that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. I submit that if a computer or storage medium is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years

later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to cloud-based storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In

addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods,

including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

34. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so

that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any

applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

CONCLUSION

35. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of the offense, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES authorizing the seizure and search of the items described in Attachment B.

Jessica Smeltz
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 19th day of April, 2019. 12:20pm

Joe L. Webster
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire premises located at 5020 Simpson Drive, Sanford, North Carolina 27330, in the county of Lee, in the Middle District of North Carolina. The house is beige and has the numbers "5020" affixed to the mailbox post at the end of the driveway. There are several outbuildings on the premises. Photographs attached.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2)(A):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);
    b. Records and information referencing child erotica;
    c. Records, information, and items referencing or revealing the occupancy or ownership of 5020 Simpson Drive, Sanford, North Carolina 27330, including utility and telephone bills, mail envelopes, or addressed correspondence;
    d. Records and information referencing or revealing the use of peer-to-peer software, including BitTorrent client software;

e. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

f. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

g. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

h. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography;

i. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

c. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of the Internet Protocol addresses used by the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

j. evidence of the lack of such malicious software;

k. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.